ABSTRACT

A formatted data structure is provided for conveying the results of ecommerce authentication programs that are used to authenticate a cardholder's on-line transactions. The data structure, which has at most a 20-byte length, is designed to be compatible with 3-D Secure message protocols used in e-commerce. The data structure includes designated fields that include a hash of the merchant's name, identify an authentication service provider, identify the authentication method used, and include a merchant authentication code which ties cardholder information to the transaction. Secure payment algorithms are provided for use by the e-commerce authentication programs to generate authentication results in the desired format. In one secure payment algorithm, a secret key is used to encrypt a concatenation of a cardholder account number with information from designated fields of the data structure. In another secure payment algorithm, a pair of secret keys is used to encrypt a concatenation of the cardholder's account number, card expiration date and service code. In both cases, portions of the encryption results are used to define the merchant authentication code.